ABSTRACT OF THE DISCLOSURE

In a secret-key cryptographic device, there are cascade-connected a plurality of round processing parts and the round processing part of each i-th round is supplied with input data L_i and R_i, nonlinearly transforms the input data R_i in a nonlinear function part on the basis of extended key, then provides the exclusive OR between the nonlinearly transformed output and the input data L_i as data R_{i+1} for input into the next round and outputs the input data R_i as data L_{i+1} for input into the next round. The nonlinear function part of each round comprises: a key-dependent linear transformation part which performs a key-dependent linear transformation of the input R_i; a splitting part which splits the linearly transformed output to four pieces of data in_0, in_1, in_2 and in_3; first nonlinear transformation parts which nonlinearly transform the four split pieces of data and output nonlinearly transformed data mid_{00}, mid_{01}, mid_{02} and mid_{03}, respectively; a key-dependent linear transformation part which associates these transformed outputs with each other and, at the same time, linearly transforms them based on extended key to output data mid_{10}, mid_{11}, mid_{12} and mid_{13}; second nonlinear transformation parts which nonlinearly transform these transformed outputs, respectively, and output data out_0, out_1, out_2 and out_3; and a combining part which combines these transformed outputs into output data Y.